# Security Advisory SWRX-2012-006

## BreakingPoint Systems Storm CTM Network Traffic Information Disclosure Vulnerability

## Dell SecureWorks Counter Threat Unit™ Threat Intelligence

### Advisory Information

**Title:** BreakingPoint Systems Storm CTM Network Traffic Information Disclosure Vulnerability
**Advisory ID**: SWRX-2012-006
**Advisory URL**: http://www.secureworks.com/research/advisories/SWRX-2012-006/
**Date published**: Wednesday, August 1, 2012
**CVE**: CVE-2012-2964
**CVSS v2 base score**: 4.8
**Date of last update**: Monday, July 23, 2012
**Vendors contacted**: BreakingPoint Systems
**Release mode**: Coordinated
**Discovered by**: Jeff Jarmoc, Dell SecureWorks

## Summary

A vulnerability exists in BreakingPoint Systems Storm CTM, which is used to test networks and data centers for resilience in the face of escalating application load and attack. The BreakingPoint Systems Storm CTM appliance and administrative Control Center graphical user interface (GUI) clients communicate in plain text. All information exchanged between client and server, including username and password, is sent in the clear. Attackers may be able to leverage this weakness by using commodity network sniffers to gather sensitive configuration information, including account credentials, session authentication tokens, test configurations, and test results.

## Affected products

BreakingPoint Systems Storm CTM V2.1.0.0 Build 71254:

http://www.breakingpointsystems.com/cyber-tomography-products/breakingpoint-storm-ctm/

Other versions may be affected, but have not been confirmed.

## Vendor information, solutions and workarounds

The vendor has not released a fix that addresses this vulnerability at publication time.

As a workaround, limit usage of the administrative GUI so that traffic traverses only trusted networks. To limit impact of potential credential exposure, ensure that unique usernames and passwords are used on affected devices.

## Details

The BreakingPoint Systems Control Center GUI administrative clients communicate in plain text. All information exchanged between client and server, including username and password, are sent in plain text XML transfers over TCP port 8880. Attackers may be able to leverage this weakness by using

commodity network sniffers to gather sensitive configuration information such as account credentials, session authentication tokens, test configurations, and test results.

BreakingPoint Systems appliances are not commonly exposed to the public Internet, which somewhat mitigates risks. The attacker must be able to sniff traffic between the client and the appliance. Successfully exploiting this vulnerability could lead to disclosure of sensitive configuration information and account credentials.

This vulnerability was first reported to the vendor on April 5, 2011. Since April 8, 2011, Dell SecureWorks Counter Threat Unit™ (CTU) researchers have been working with members of the CERT® Coordination Center (CERT/CC), who have been coordinating disclosure with the vendor. Although originally stating that a fix would be available by fall 2011, the vendor delayed the release several times. The latest information is that the vulnerability will be addressed in version 3.0, scheduled for release by August 6, 2012.

## CVSS severity (version 2.0)

**Access Vector:** Adjacent network; exploitable from networks in the client-server communications flow
**Access Complexity:** Low
**Authentication:** Not required to exploit
**Impact Type:** Information disclosure
**Confidentiality Impact:** Partial
**Integrity Impact:** Partial
**Availability Impact:** None
**CVSS v2 base score**: 4.8
**CVSS v2 impact subscore**: 4.9
**CVSS v2 exploitability subscore**: 6.5
**CVSS v2 vector**: (AV:A/AC:L/Au:N/C:P/I:P/A:N)

## Proof of concept

Commodity packet sniffers can be used to intercept data between the client and the server on port 8880. Example:

```
<login token="#loginData" locale="en" password="REDACTED" id="REDACTED"/>.<com
type="reply" token="#loginData" status="ok" timeTaken="0.050609995"><ok version-
primary="2.1.0.0" strikepack-primary="0.9" revision-primary="71254" strikerev-
primary="75591" version-backup="2.1.0.0" revision-backup="71254" strikepack-
backup="0.9" strikerev-backup="71254" version-factory="2.1.0.0" revision-
factory="71254" strikepack-factory="0.9" strikerev-factory="71254" serialno="REDACTED"
bpsh_version="71084" updateAvailable="false" updateDescription=""
strikepackAvailable="false" strikepackDescription="" systemType="Storm CTM"
jsessionid="F24BF6E06EC9F94D26934D09B1406A92"
sessionid="FD3B336D1F7D6D7336AF4ACEFFB94555" schemaver="201" /></com>.<getResource
token="#welcomeModuleLabelsAndMenus" name="main" type="module"/>.<getOpenMRU
token="#gatherRecentlyOpen"/>.<getRunMRU token="#gatherRecentlyRun"/>.<userInfo
token="#getFullUserData" id="REDACTED"/>.<getUserPref
token="#gatherUserPrefs"/>.<getSystemGlobals token="#getSystemGlobals"/>.<networkInfo
token="#getRoute"/>.<getOutputs token="#getOutputs"/>.<com type="reply”
token="#welcomeModuleLabelsAndMenus" status="ok" timeTaken="0.00621748"><resource
type="module" name="main"><labels>
```

Red indicates client to server transmissions, while black indicates server to client replies.

## Revision history

1.0 2012-08-01: Initial advisory release

## PGP keys

This advisory has been signed with the Dell SecureWorks Counter Threat Unit PGP key, which is available for download at http://www.secureworks.com/contact/SecureWorksCTU.asc.

## About Dell SecureWorks

Dell Inc. (NASDAQ: DELL) listens to customers and delivers worldwide innovative technology and business solutions they trust and value. Recognized as an industry leader by top analysts, Dell SecureWorks provides world-class information security services to help organizations of all sizes protect their IT assets, comply with regulations and reduce security costs.

## Disclaimer